Kyle McLean (SBN #330580)
Email: kmclean@sirillp.com
Mason Barney*
Email: mbarney@sirillp.com
Tyler Bean*
Email: tbean@sirillp.com
SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: 213-376-3739

Attorneys for Plaintiff and the Nationwide Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

LISA MIKEC, on behalf of herself and all others similarly situated, Plaintiff, v. BLACKHAWK NETWORK, INC. d/b/a BLACKHAWK ENGAGEMENT SOLUTIONS, Defendant.	Case No. **CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiff Lisa Mikec, individually and on behalf of the Class defined below of similarly situated persons ("Plaintiff"), alleges the following against Blackhawk Network, Inc. d/b/a Blackhawk Engagement Solutions ("Blackhawk" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters. This Court has jurisdiction over Defendant because Defendant operates and has its principal place of business in this District, and the

computer systems implicated in this Data Breach are likely based in and/or controlled in this District.

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated customers' payment card information and other sensitive records as part of a computer hack that Defendant's lax data security practices permitted to occur.

2. Upon information and belief, Blackhawk acts as a third-party service provider on behalf of Pathward N.A. ("Pathward") and other entities. Pathward uses Blackhawk to activate and manage certain prepaid incentive cards referred to as Pathward Prepaid Cards ("Prepaid Card(s)").

3. Blackhawk operates the website www.MyPrepaidCenter.com ("MyPrepaidCenter.com") on behalf of Gift Card holders to activate and manage Pathward's Prepaid Cards. To purchase and use Prepaid Cards, Plaintiff and Class Members were required to provide certain sensitive, non-public information to Defendant by entering this information on MyPrepaidCenter.com.

4. However, on August 12, 2023, Defendant was alerted to unusual activity on certain of MyPrepaidCenter.com. Specifically, Defendant asserts that unauthorized parties used a malicious exploit on the website that provided access to certain customer payment card information, including that belonging to Plaintiff and Class Members, between June 16, 2023, and August 19, 2023 (the "Data Breach"). This is the second data breach of a similar effect that has impacted Defendant within a year's time, with the first occurring on MyPrepaidCenter.com in September of 2022.

5. Affected information includes customer names and payment card information such as card numbers, expiration dates, and CVV codes (the "Private Information") required by Blackhawk and provided by customers (including Plaintiff) for the chance to purchase and use prepaid cards.

6. On or about September 27, 2023, Defendant filed a data breach notice with the California Attorney General's office.[1]

7. On or about that same day, Defendant began notifying affected individuals, including Plaintiff. As of the date of this filing, there is no mention of the data breach on Defendant's website. This means that Plaintiff and Class Members had no idea their private information had been compromised for almost two months after Defendant knew or should have known, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. Defendant's Notice of Data Breach Letters (the "Notice Letter") disclosed information regarding the data breach. Based on just the details in those letters it appears that the information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, such as customer name, payment card number, expiration date, and CVV number (collectively the "Private Information") and, on information and belief, potentially additional personally identifiable information ("PII") that Defendant collected and maintained.

9. Armed with the Private Information accessed in the Data Breach, and a one-month head start, data thieves can commit a variety of crimes including, *e.g.*, making fraudulent purchases and committing identity theft such as opening new financial accounts in Class Members' names.

10. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class

[1] *See California Office of Attorney General* website, https://oag.ca.gov/ecrime/databreach/reports/sb24-574287; *see also Sample of Notice Letter*, https://oag.ca.gov/system/files/BHN%20Customer%20Notification%20Letter.pdf

Members must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Defendant also failed to offer any amount of credit monitoring services; therefore, Plaintiff and Class Members will be forced to incur out of pocket costs for, *e.g.,* purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. Thus, Plaintiff and Class Members have already suffered and/or are at a heightened and continuous risk of suffering, ascertainable losses in the form of the fraudulent misuse of their Private Information, the loss of the benefit of their bargain made with Blackhawk, out-of-pocket expenses dealing with and mitigating the direct impact of the Data Breach on their lives, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

13. Plaintiff brings this class action lawsuit to address Defendant's continual inadequate safeguarding of Class Members' Private Information that it collected and maintained.

14. The potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, especially in light of the previously reported data breach, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

15. Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its website, it would have discovered the Data Breach sooner and likely could have prevented it from occurring.

16. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct leading to the Data Breach.

17. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

18. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including long-term improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

19. Plaintiff therefore brings claims of negligence, negligence per se, breach of contract, breach of implied contract, unjust enrichment, and declaratory judgement.

PARTIES

20. Plaintiff Lisa Mikec is, and at all times mentioned herein was, an individual citizen of the State of Pennsylvania.

21. Blackhawk Network, Inc. d/b/a Blackhawk Engagement Solutions is, and all times mentioned herein was, a privately held corporation incorporated in the State of California. Defendant's headquarters are located at 6220 Stoneridge Mall Road, Pleasanton, California 94588. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

JURISDICTION AND VENUE

22. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

23. This Court has jurisdiction over the Defendant because it operates and has its principal place of business in this District, and the computer systems implicated in this Data Breach are likely based in and/or controlled in this District.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Background

25. Blackhawk is primarily engaged in providing "global branded payments" to its customers located within the United States and abroad, which includes gift cards, prepaid incentive cards, other online payment options for employer and merchants, gaming, and gambling options.[2] Blackhawk is a privately held company with corporate headquarters in Pleasanton, California.

26. Blackhawk operates a consumer facing website located at www.blackhawknetwork.com ("Blackhawknetwork.com"). Customers or potential customers can then access MyPrepaidCenter.com through Blackhawknetwork.com.

27. To activate or access a prepaid card on MyPrepaidCenter.com a customer must provide certain Private Information. It is specified in the Blackhawk Network Privacy Notice ("Privacy Notice") that the policy pertains to all visitors, customers, users of apps, and users of gift card and banded payments. Specifically, the Private Information, which Defendant collects, includes, but is not limited to:

- Contact information, such as name, email address, mailing address, fax, or phone number;
- Payment and financial information, such as credit or other payment card information, bank account, or billing address;
- Shipping address and related details;

[2] Blackhawk Network Website, *available at:* https://blackhawknetwork.com/ (last accessed on Oct. 3, 2023).

- Resume, employment and education history, name and contact details, background details, and references when you apply to job postings or contact defendant about employment opportunities;
- Company and employment information;
- Subject to applicable local law restrictions, Social Security number or other national tax ID number (for clients and potential clients);
- Unique identifiers such as username, account number, or password;
- Preference information such as product wish lists, order history, or marketing preferences;
- Information about businesses, such as company name, size, or business type; and
- Demographic information, such as age, gender, interests, and ZIP or postal code.[3]

28. Defendant also specifies in the Privacy Policy that it acts as the "Controller" of the Private Information supplied.

29. When they provided their information to Defendant, Plaintiff and Class Members relied on Defendant (a large, sophisticated internet retailer) to keep it confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

30. Defendant had a duty to take reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to unauthorized third parties. This duty is inherent in the nature of the exchange of the highly sensitive Private Information at issue here, particularly where digital transactions are involved.

31. Defendant also recognized and voluntarily adopted additional duties to protect PII and payment card data in its Privacy Policy which has been publicly posted to

[3] *Blackhawk Network Privacy Notice*, quoting, "Personal Information we Collect" *available at*: https://blackhawknetwork.com/privacy-policy (last accessed on Oct. 3, 2023).

the internet. In its Privacy Policy, Defendant also says the way it uses Private Information is at the "core of our obligations," that it will "not sell" information, and that it will use the information for "our own legitimate and lawful business interests."[4]

32. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

The Data Breach was Foreseeable

33. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[5]

34. In light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information it collected and maintained would be targeted by cybercriminals.

35. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and may therefore take appropriate measures to prepare for (or thwart) such an attack.

36. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgement of its duties to keep Private Information confidential and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and the Class from being compromised.

The Data Breach

[4] *Blackhawk Network Privacy Notice*, quoting, "Personal Information we Collect" *available at*: https://blackhawknetwork.com/privacy-policy (last accessed on Oct. 3, 2023).

[5] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-

37. On or about September 27, 2023, Defendant notified the California Attorney General, as well as Plaintiff and Class Members that, on August 19, 2023, Defendant discovered that MyPrepaidCenter.com experienced "irregular activity."

38. The Notice informed Plaintiff and Class Members that, "Our investigation revealed that irregular activity involved the unauthorized acquisition of information about you." This information included name and payment card information including card number, expiration date, and CVV code.

39. The Private Information exfiltrated in the Data Breach was unencrypted and captured directly from MyPrepaidCenter.com.

40. Defendant claims it "blocked your impacted Pathward Prepaid Card(s)," yet it remained silent about what happened to the stolen Private Information.

41. Despite Defendant's promises that it: (i) would not disclose consumers' Private Information to unauthorized third parties; and (ii) would protect consumers' Private Information with adequate security measures, it appears that Defendant did not even implement, or require its third-party vendors to implement, basic security measures such as immediately encrypting payment card data. This negligence imposes risks to Plaintiff and Class Members that they must endure for the foreseeable future.

Blackhawk Experienced a Substantially Similar Date Breach One Year Earlier

42. According to an earlier Security Incident Notification ("Notification"), Blackhawk "discovered irregular activity in connection with www.myprepaidcenter.com" in or around late October of 2022.

43. Blackhawk's investigation revealed that the irregular activity involved unauthorized acquisition of personal information of individuals.

44. The Notification also indicates similar Private Information was taken in the 2022 data breach as was taken in the Data Breach that is the subject of this class action, including name and payment card information.

DEFENDANT FAILED TO COMPLY WITH FTC GUIDELINES

45. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

46. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

47. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. On information and belief, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

50. Defendant was at all times fully aware of its obligation to protect the PII of its customers.

DEFENDANT FAILED TO COMPLY WITH INDUSTRY STANDARDS

51. Experts studying cyber security routinely identify ecommerce platforms as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

52. Several best practices have been identified that a minimum should be implemented by ecommerce providers like Defendant, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

53. A number of industry and national best practices have been published and should be used as a go-to resource when developing a business' cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls. The CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia.[6]

54. Other best cybersecurity practices that are standard in the ecommerce industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems;

[6] *CIS Benchmarks FAQ*, Center for Internet Security, *available at* https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq (last visited August 10, 2022).

setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

55. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

FBI, FTC, NIST GUIDELINES ON PROTECTING CUSTOMER PERSONAL INFORMATION

56. Recently, the FBI issued a warning to companies about this exact type of fraud. In the FBI's Oregon FBI Tech Tuesday: Building a Digital Defense Against E-Skimming, dated October 22, 2019, the agency stated:

> This warning is specifically targeted to . . . businesses . . . that take credit card payments online. E-skimming occurs when cyber criminals inject malicious code onto a website. The bad actor may have gained access via a phishing attack targeting your employees—or through a vulnerable third-party vendor attached to your company's server.[7]

57. The FBI gave some stern advice to companies like Defendant:

> Here's what businesses and agencies can do to protect themselves:
>
> - Update and patch all systems with the latest security software.
> - Anti-virus and anti-malware need to be up-to-date and firewalls strong.
> - Change default login credentials on all systems.

[7] https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-agaist-e-skimming

- Educate employees about safe cyber practices. Most importantly, do not click on links or unexpected attachments in messages.
- Segregate and segment network systems to limit how easily cyber criminals can move from one to another.

58. But Defendant apparently did not take this advice in 2022 and, now, more recently, because hackers scraped customers' Private Information off its website for months until Defendant was able to cease the unauthorized access.

59. Similarly, the Federal Trade Commission ("FTC") has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act (codified by 15 U.S.C. § 45).

60. Under the FTC Act, Defendant is prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

61. Beginning in 2007, the FTC released a set of industry standards related to data security and the data security practices of businesses, called "Protecting Personal Information: A Guide for Businesses" (the "FTC Guide"). In 2011, this guidance was updated to include fundamental data security principles for businesses. In addition to the necessity to protect consumer data, the guide established that:

- Businesses should dispose of personal identifiable information that is no longer needed;
- Businesses should encrypt personal identifiable information and protected cardholder data stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- Businesses should thoroughly understand the types of vulnerabilities on their network (of which malware on a

point-of-sale system is one) and how to address said vulnerabilities;

- Businesses should implement protocols necessary to correct security breaches;
- Businesses should install intrusion detection systems to expose security breaches at the moment they occur;
- Businesses should install monitoring mechanisms to watch for massive troves of data being transmitted from their systems; and,
- Businesses should have an emergency plan prepared in response to a breach.

62. On information and belief, Defendant failed to adequately address the foregoing requirements in the FTC Guide.

63. In 2015, the FTC supplemented the FTC Guide with a publication called "Start with Security" (the "Supplemented FTC Guide"). This supplement added further requirements for businesses that maintain customer data on their networks:

- Businesses should not keep personal identifiable information and protected cardholder data stored on their networks for any period longer than what is needed for authorization;
- Businesses should use industry-tested methods for data security; and,
- Businesses should be continuously monitoring for suspicious activity on their network.

64. Again, Defendant apparently failed to adequately address these requirements enumerated in the Supplemented FTC Guide.

65. The FTC Guide is clear that businesses should, among other things: (1) protect the personal customer information they acquire; (2) properly dispose of personal information that is no longer needed; (3) encrypt information stored on computer networks; (4) understand their network's vulnerabilities; and (5) implement policies for installing vendor-approved patches to correct security vulnerabilities. The FTC guidance

also recommends that businesses: (1) use an intrusion detection system to expose a breach as soon as it occurs; (2) monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and (3) watch for large amounts of data being transmitted from the system. Plaintiff believes that Defendant did not follow these recommendations, and as a result exposed hundreds of thousands of consumers to harm.

66. Furthermore, the FTC has issued orders against businesses for failing to employ reasonable measures to safeguard customer data. The orders provide further public guidance to businesses concerning their data security obligations.

67. Defendant knew or should have known about its obligation to comply with the FTC Act, the FTC Guide, the Supplemented FTC Guide, and many other FTC pronouncements regarding data security.

68. Thus, among other things, Defendant's misconduct violated the FTC Act and the FTC's data security pronouncements, which led to the Data Breach, and resulted directly and proximately in harm to Plaintiff and Class Members.

69. Additionally, the National Institute of Standards and Technology (NIST) provides basic network security guidance that enumerates steps to take to avoid cybersecurity vulnerabilities. Although use of NIST guidance is voluntary, the guidelines provide valuable insights and best practices to protect network systems and data.

70. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.

71. Defendant's failure to protect massive amounts of Payment Information throughout the multi-month breach period belies any assertion that Defendant employed proper data security protocols or adhered to the spirit of the NIST guidance.

DEFENDANT'S SECURITY OBLIGATIONS

72. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to fully comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

e. Failing to adhere to industry standards for cybersecurity.

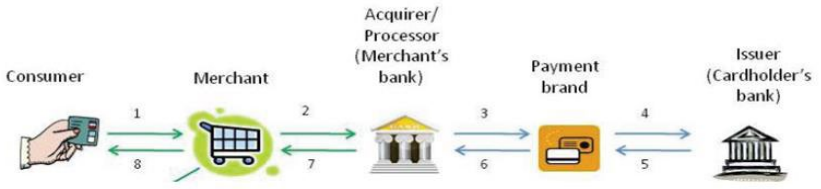
73. On information and belief, as the result of computer systems in need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

74. Accordingly, as outlined below, Plaintiff's and Class Members' daily lives were severely disrupted. What's more, Plaintiff has already experienced (and Plaintiff and Class Members now face an increased risk of) fraud and identity theft as a direct result of the Data Breach. Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant as its customers.

DATA BREACHES, FRAUD AND IDENTITY THEFT

75. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to an e-commerce retailer (through an e-commerce website) to pay for

merchandise. The card is then "swiped" and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (i.e., the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (i.e., cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction. See graphic below:[8]



1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

76. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

77. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain

[8] "Payments 101: Credit and Debit Card Payments," (First Data) *available at http://euro.ecom.cmu.edu/resources/elibrary/epay/Payments-101.pdf* (last visited October 27, 2022); *see also* "Payments 101: An Intro to Card Networks and Card Transactions" (Very Good Security), *available at https://www.verygoodsecurity.com/blog/posts/payments-101-an-intro-to-card-networks-and-card-transactions* (last visited October 27, 2022).

text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment it is "swiped," hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the cardholder's personal information stored in the retailer's computers.

78. However, when the data is not encrypted, hackers can target what they refer to as the *fullz*–a term used by criminals to refer to stealing the full primary account number, card holder contact information, credit card number, CVC code, and expiration date. The *fullz* is exactly what appears to have been scraped from Defendant's ecommerce platform. Typically, these hackers insert virtual credit card skimmers or scrapers (also known as *formjacking*) into a web application (usually the shopping cart) and proceed to scrape credit card information to sell on the dark web.[9]

79. At the very least, Defendant once again chose not to invest in the technology to encrypt payment card data at point-of-sale to make its customers' data more secure, despite already having just experienced a similar data breach only months before. Upon information and belief, Defendant also failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach, and/or failed to provide sufficient control employee credentials and access to computer systems to prevent a security breach and/or theft of payment card data.

80. The FTC hosted a workshop to discuss "informational injuries" which are injuries that consumers suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data.[10] Exposure of personal information that a consumer wishes to keep private may cause both market and non-market harm to the consumer, such as the ability to obtain or keep employment and negative impact on consumer's

[9] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost (August 28, 2019), *available at*: https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/.

[10] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

relationships with family, friends, and coworkers. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

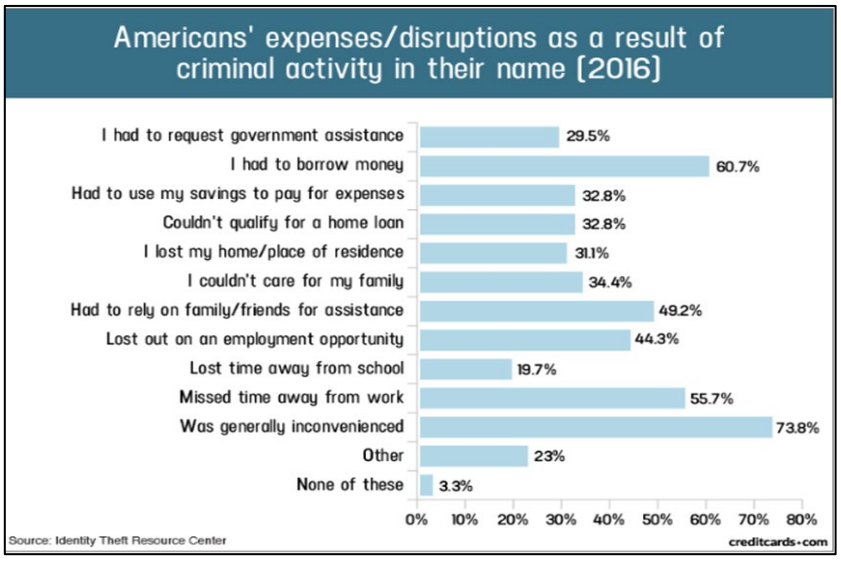
81. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

82. The detailed information potentially obtained in the instant data breach regarding the nature of the purchases Plaintiff and Class Members made on the Blackhawk website makes the risk of phishing attacks even greater. With detailed purchase information, criminals will be able to reference those specific purchases that Plaintiff and Class Members will recognize, making it harder for Plaintiff and Class Members to identify such phishing attacks.

83. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting

companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

84. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII:[12]



85. Moreover, theft of Private Information is also gravely serious. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

86. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the

[11] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited August 11, 2022).

[12] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/.

U.S. Government Accountability Office, which conducted a study regarding data breaches:[13]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

87. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

88. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

89. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

90. Plaintiff's Private Information, including her sensitive payment card data, was compromised as a direct and proximate result of the Data Breach.

91. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

92. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unkno˙wn*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html.

93. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

94. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, along with other similar costs directly or indirectly related to the Data Breach, especially considering the fact that Defendant failed to offer any such relief.

95. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for.

96. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

97. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

98. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and either have suffered harm or are at an imminent and increased risk of future harm.

CLASS ACTION ALLEGATIONS

99. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and on behalf of all other persons similarly situated.

100. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **Nationwide Class** (the "Class")
> All individuals in the United States whose Private Information was subject to the Data Breach announced by Defendant on or about September 27, 2023, including those who Defendant identified as being among those individuals impacted by the Data Breach, and all persons who were sent a notice of the Data Breach.

101. Excluded from the above Class are Defendant and their parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

102. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

103. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

104. Numerosity**.** The Class Members are so numerous that joinder of all members is impracticable. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

105. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;
b. When Defendant actually learned of the data breach and whether its response was adequate;
c. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;
d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
f. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
g. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
h. Whether Defendant breached their duty to Class Members to safeguard their Private Information;
i. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
j. Whether Defendant had a legal duty to provide timely and accurate notice of the data breach to Plaintiff and Class Members;
k. Whether Defendant breached its duty to provide timely and accurate notice of the data breach to Plaintiff and Class Members;
l. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
m. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant was unjustly enriched;

p. Whether Plaintiff and Class Members are entitled to credit or identity monitoring and are entitled to other monetary relief; and

q. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

106. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

107. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

108. Predominance**.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

109. Superiority**.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct

of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

110. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Defendant has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

111. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

112. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

113. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

114. Defendant knew, or should have known, of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security, especially in light of its recent data security issues that have now resulted in at least two major data breaches within the last year.

115. Defendant owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to them. Defendant's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to California law (where Defendant is headquartered), specifically the Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.;*

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to disclose precisely the type(s) of information compromise.

116. Plaintiff and Class Members were foreseeable and probable victims of any inadequate security practices, and Defendant owed them a duty of care not to subject them to an unreasonable risk of harm.

117. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

118. Defendant, by its actions and/or omissions, breached its duty of care by failing to provide, or by acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

119. Defendant, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

120. Defendant acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach so that they could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

121. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate data security precautions. Moreover, only Defendant had the ability to protect its systems (and the Private Information that it stored thereon) from unauthorized access and disclosure.

122. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

123. Defendant's breaches of duty caused a foreseeable risk of harm to Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

124. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, and which, in Plaintiff's case, has already been misused for fraudulent purposes.

125. Defendant also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

126. But for Defendant's wrongful and negligent breach of the duties it owed Plaintiff and Class Members, their Private Information either would not have been compromised or they would have been able to prevent some or all of the damages alleged herein to have been suffered.

127. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of further harm.

128. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was reasonably foreseeable.

129. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct.

130. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

131. In addition to monetary relief and in light of Defendant's recent data breaches, Plaintiff and Class Members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

132. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

133. Plaintiff and Class Members entered into a valid and enforceable contract when they paid money to Defendant in exchange for services, which included promises

to secure, safeguard, protect, keep private, and not disclose Plaintiff's and Class Members' Private Information.

134. Defendant's Privacy Policy memorialized the rights and obligations of Defendant and its customers. This document was provided to Plaintiff in a manner and during a time when it became part of the agreement for services.

135. In the Privacy Policy, Defendant commits to protecting the privacy and security of private information and promises to never share customer information aside from limited exceptions.

136. Plaintiff and Class Members fully performed their obligations under their contracts with Defendant.

137. Defendant did not secure, safeguard, protect, and/or keep private Plaintiff's and Class Members' Private Information and/or it disclosed their Private Information to third parties, and therefore Defendant breached its contract with Plaintiff and Class Members.

138. Defendant allowed third parties to access, copy, and/or transfer Plaintiff's and Class Members' Private Information, without permission, and therefore Defendant breached its contracts with Plaintiff and Class Members.

139. Defendant's failure to satisfy its confidentiality and privacy obligations resulted in Defendant providing services to Plaintiff and Class Members that were of diminished value.

140. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein.

141. In addition to monetary relief and in light of Defendant's recent data security issues resulting in two major data breaches in the last two years, Plaintiff and Class Members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits

of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

142. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

143. Plaintiff brings this Count alternatively to Count II above.

144. Defendant provides ecommerce services to Plaintiff and Class Members. Plaintiff and Class Members also formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for services and/or receiving goods in the form of event tickets from Defendant.

145. Through Defendant's performance, sale, and/or purchase of goods and services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Personal Information in accordance with Defendant's policies, practices, and applicable law.

146. As consideration, Plaintiff and Class Members paid money to Defendant for goods and turned over their valuable Private Information to Defendant. Accordingly, Plaintiff and Class Members bargained with Defendant to securely maintain and store their Private Information.

147. Defendant violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information and by allowing the disclosure of said Private Information for purposes not required or permitted under the contracts or agreements.

148. Plaintiff and Class Members have been damaged by Defendant's conduct, including by paying for data and cybersecurity protection that they did not receive, as

well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

149. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

150. This count is pled in the alternative to Counts II and III above.

151. Plaintiff and Class Members conferred a benefit on Defendant by paying for data and cybersecurity procedures to protect their Private Information that they did not receive.

152. Defendant has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to Defendant's conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendant to be permitted to retain the benefit of their wrongful conduct.

153. Plaintiff and Class Members are entitled to full refunds, restitution and/or damages from Defendant and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. If necessary, the establishment of a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation may be created.

154. Additionally, Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly plead this claim for unjust enrichment in addition to or, in the alternative to, other claims pleaded herein.

COUNT V
DECLARATORY/INJUNCTIVE RELIEF
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

155. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

156. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

157. Defendant owes a duty of care to Plaintiff and Class Members which required it to adequately secure Private Information.

158. Defendant still possesses Private Information regarding Plaintiff and Class Members.

159. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and remains at imminent risk that further compromises of her Private Information will occur in the future.

160. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

161. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect customers' Private Information, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order Defendant to comply with its explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and securing checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and

contain a breach when it occurs and what to do in response to a breach;

vii. meaningfully educating its users about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

162. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

163. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued, especially considering the Data Breach is the second breach of Defendant's network and systems in less than two years. Therefore, Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by finally employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

164. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and customers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seeks the following relief:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class

Counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury as to all triable issues.

Dated: October 4, 2023,

Respectfully submitted,

By: */s/ Kyle McLean*

Kyle McLean (SBN #330580)
Email: kmclean@sirillp.com
Mason Barney*
Email: mbarney@sirillp.com
Tyler Bean*
Email: tbean@sirillp.com

SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: 213-376-3739

Attorneys for Plaintiff and the Proposed Class

**Pro Hac Vice Applications Forthcoming*